

Express Mail Label No. EV 318 174 393 US

Date of Mailing: September 30, 2003

PATENT
Case No. CE11461JDP
(9640/130)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR UNITED STATES LETTERS PATENT

INVENTOR(S): BRIAN K. SMITH
 FLOYD D. SIMPSON
 TIMOTHY J. WILSON

TITLE: ENHANCED PASSIVE SCANNING

ATTORNEYS: MOTOROLA, INC.
 INTELLECTUAL PROPERTY - DOCKETING
 1303 E. ALGONQUIN ROAD
 IL01 – 3RD FLOOR
 SCHAUMBURG, IL 60196
 (847) 538-2450

ENHANCED PASSIVE SCANNING

5

FIELD OF THE INVENTION

This invention relates generally to methods of operating wireless communication systems and wireless local area networks. More specifically, the invention relates to scanning methods for establishing communications between
10 a mobile station and an access point.

BACKGROUND OF THE INVENTION

Wireless local area networks (WLANs) typically transmit via radio or infrared frequencies to connect data devices. In a WLAN, the wireless
15 communication devices are often mobile, moving around more or less freely within the networked area. WLANs combine with infrastructure networks systems that can be connected to the Internet, thereby providing communication over long distances.

WLANs link portable and wireless computer devices, also called mobile
20 stations or terminals, to a wired LAN via a plurality of fixed access points (APs), also called base stations. Allowing WLAN devices to communicate with the infrastructure network, access points provide for wireless communications within respective cells and are typically spaced throughout a designated networked area. The access points facilitate communications between a networked set of
25 802.11-compliant devices called a basic service set (BSS), as well as communications with other BSSs and wired devices in or connected to wired infrastructure network systems.

WLANs have been used in proprietary business applications such as order entry, shipping, receiving, package tracking, inventory, price-markdown verification, and portable point of sale. Such systems may have an operator
5 carrying a handheld computer device that communicates with a server via one or more access points such as a wireless bridge or router, each access point interacting with the server to create a wireless cell.

The most common WLAN technologies are described in the Institute of Electrical and Electronics Engineer's IEEE 802.11 family of industry
10 specifications, which include two physical-layer standards: 802.11b operating at 2.4GHz and delivering up to 11Mbps at 250 feet maximum; and 802.11a operating at 5GHz and delivering up to 54Mbps at 150 feet maximum. A third standard, 802.11g, provides the speeds of 802.11a at the distances of 802.11b. IEEE 802.11 specifies Carrier Sense Multiple Access with Collision Avoidance
15 (CSMA/CA) for devices operating within an 802.11 wireless network. Informative material may be found in IEEE Std. 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, reference number ISO/IEC 8802-11:1999, ANSI/IEEE Std. 802.11, 1999 edition, 1999.

When a wireless devices moves around a WLAN, it may need to change
20 its association from one access point to another if the reception level of the associated access point becomes too low. The procedure known as roaming allows a WLAN device to switch between access points, a change that is generally based on the relative reception levels of the access points involved. Roaming procedures may be based on selected configuration settings for the
25 access points (APs) such as density levels of cell sizes that influence their defer, carrier-detect, and cell-search behaviors.

Within the wireless networks, wireless communications are generally managed according to an operating protocol that requires ongoing wireless activity to monitor the roaming of WLAN devices and to synchronize radio timing between these portable devices and access points. This ongoing activity contributes to the draining of power from battery-powered WLAN devices. Synchronization of radio timing becomes especially critical in the management of wireless communications, and more efficient scheduling of future coordinated activities provides better power-saving strategies.

10 Before a WLAN device can communicate with other devices in a given WLAN, it must first locate access points. The medium access control (MAC) layer-2 protocol of the IEEE 802.11 manages, coordinates and maintains communications, traffic, and data distribution in wireless networks that have fixed access points or in ad hoc networks. The IEEE 802.11 MAC protocol defines
15 beacon frames sent at regular intervals, known as beacon intervals, for example, every 100 microseconds, by an access point that allow WLAN devices to monitor for the presence of an access point. Passive and active scanning techniques have been developed for WLAN devices to detect access points, although the 802.11 standard does not mandate particular methods for scanning.

20 Passive scanning allows the network interface card (NIC) of a WLAN device to find an IEEE 802.11 network by listening for traffic. As defined in 802.11, passive scanning involves a WLAN device listening to each frequency channel for no longer than a maximum duration defined by the ChannelTime parameter. In this passive mode, the wireless NIC listens for beacons from
25 neighboring access points, while extracting information about the particular channel. Passive scanning expends time and battery power while listening for a beacon frame that may never occur or may be on an idle channel.

The ChannelTime is configured during the initialization stage of the WLAN device driver. To initiate a passive scan, the driver commands the firmware to perform a passive scan with a list of channels. The firmware sequences through the list of channels and sends any received frames to the driver. The amount of time spent on the channel is equal to the ChannelTime value. The driver is able to abort the passive scan when the desired beacon or probe response is received.

Active scanning, in contrast to passive scanning, requires the scanning wireless NIC to transmit requests and receive responses from other 802.11 wireless NICs and access points. Active scanning allows the mobile wireless NIC to interact with another wireless NIC or access point based on probe requests and probe responses.

The active scanning of the IEEE 802.11 MAC uses a set of management frames including probe request frames that are sent by a WLAN device and are followed by probe response frames sent by an available access point. In this way, a WLAN device may scan actively to locate an access point operating on a certain channel frequency and the access point can indicate to the WLAN device what parameter settings it is using.

In an active scan, the WLAN device transmits a probe request frame, and if there is a network on the same channel that matches the service set identity (SSID) in the probe request frame, an access point in that network will respond by sending a probe response frame to the WLAN device. The probe response includes information the WLAN device uses to access a description of the network. The WLAN device processes the beacon frames and any additional probe responses that it may receive.

Once the various responses are processed or it has been determined that no response has been received within a prescribed time, a WLAN device may continue to scan on another radio channel. At the end of the scanning process, the WLAN device has accumulated data about the networks in its vicinity, and the device can determine which network to join. When compared to passive scanning, active scanning results in longer battery life for the WLAN device, but it also reduces network capacity.

After passive or active scanning, a WLAN device registers itself with the AP of the chosen network, synchronizes with the AP and, thereafter, transmits and receives data to and from the AP. According to the IEEE 802.11 standard, the registration includes an authentication whereby the AP identifies whether a WLAN device has the right or not to access the wireless network via a medium access control (MAC) layer. Generally, this authentication phase requires bi-directional authentication steps with the AP and WLAN device exchanging some packets, and optionally, may include additional steps of assertion of identity, challenge of assertion, and response to challenge. After authentication, the WLAN device establishes a connection link with the AP by sending an association request packet to the AP and waiting to receive a response frame from the AP that acknowledges the association. The WLAN device joins a basic service set (BSS) by setting its local hopping time and channel sequence according to the information contained in the AP beacon.

The AP is the timing master of the network, performing a TSF (timing synchronization function) to keep the timers for all WLAN devices synchronized within the same basic service set (BSS) of a larger network. The beacons that are broadcast at fixed time intervals by the AP contain copies of the TSF timer and hopping sequence to synchronize other WLAN devices in a BSS. When a timestamp of a device's TSF timer is different from the timestamp in the received beacon frame, the WLAN device resets its timestamp value to match the received timestamp value.

The total time that is consumed for devices using IEEE 802.11 WLAN and other wireless communication technologies to complete all the steps of scanning, authentication and association can vary greatly. Thus, improving the scanning process for wireless networks would help the establishment of a connection between devices and the communication within a network to become more predictable, as well as to become more power and time efficient, particularly for battery-powered IEEE 802.11 WLAN devices. More effective programming techniques for scanning would minimize the number of probe requests generated, the amount of time the receiver of the device is set to an on-state, and the number of times the firmware is interrupting a host controller for beacon processing. Thus, the improved scanning system would increase the battery life of a WLAN device, because the device would need less time to scan or monitor for beacon signals from a primary as well as neighboring access points. In addition, improvements of the scanning system for a WLAN network would benefit associated networks such as wide area networks (WAN), personal area networks (PAN), and controller area networks (CAN).

SUMMARY OF THE INVENTION

One aspect of the invention provides an enhanced passive scanning method for a wireless local area network. At least one of a beacon signal or a gratuitous probe response is received. A site timing table entry in a site timing table is updated based on the received beacon signal or gratuitous probe response. A scan start time is set based on entries in the updated site timing table, and then a power mode for a wireless communication device is determined based on the scan start time.

Another aspect of the invention provides an enhanced passive scanning system for a wireless local area network, including means for receiving at least one of a beacon signal or a gratuitous probe response, means for updating a site timing table entry in a site timing table based on the received beacon signal or gratuitous probe response, means for setting a scan start time based on entries

in the updated site timing table, and means for determining a power mode for a wireless communication device based on the scan start time.

Another aspect of the invention provides a computer usable medium including a program for enhanced passive scanning for a wireless local area network. The program includes computer program code to receive at least one of a beacon signal or a gratuitous probe response, computer program code to update a site timing table entry in a site timing table based on the received beacon signal or gratuitous probe response, computer program code to set a scan start time based on entries in the updated site timing table, and computer program code to determine a power mode for a wireless communication device based on the scan start time.

The present invention is illustrated by the accompanying drawings of various embodiments and the detailed description given below. The drawings should not be taken to limit the invention to the specific embodiments, but are for explanation and understanding. The detailed description and drawings are merely illustrative of the invention rather than limiting, the scope of the invention being defined by the appended claims and equivalents thereof. The foregoing aspects and other attendant advantages of the present invention will become more readily appreciated by the detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of the present invention are illustrated by the accompanying figures, wherein:

FIG. 1 illustrates an enhanced passive scanning system for a wireless local area network, in accordance with one embodiment of the current invention;

FIG. 2 illustrates an enhanced passive scanning system for a wireless local area network, in accordance with another embodiment of the current invention;

FIG. 3 is a plot of beacon signals and gratuitous probe responses transmitted from two access points, in accordance with one embodiment of the current invention;

FIG. 4 is a flow diagram of an enhanced passive scanning method for a wireless local area network, in accordance with one embodiment of the current invention;

FIG. 5 is a block diagram of an enhanced passive scanning system for a wireless local area network, in accordance with one embodiment of the current invention; and

FIG. 6 is a block diagram of an enhanced passive scanning system for a wireless local area network, in accordance with another embodiment of the current invention.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENTS

FIG. 1 shows an enhanced passive scanning system for a wireless local area network (WLAN), in accordance with one embodiment of the present invention at **100**. WLAN **100** includes one or more wireless communication devices referred to herein as mobile stations **110**, **112**, **114** and **116**, and one or more access points **120** and **124**. Access points **120** and **124** may be connected to an infrastructure network **130**, which in turn may be connected to other wired and wireless networks (not shown). Mobile stations **110**, **112**, **114** and **116** include radio transmitters and receivers for transmitting and receiving signals such as voice over IP, data packets, control frames, and network management frames. Mobile stations **110**, **112**, **114** and **116** can communicate wirelessly with access points **120** and **124**, and can be set to communicate with each other. In one embodiment, two mobile stations **110** and **112** form an ad hoc network with the ability to establish communications when in close proximity to each other. Often, one or more mobile stations **110**, **112** and **114** will connect wirelessly to an access point **120**, using standardized protocols such as IEEE 802.11, commonly referred to as Wi-Fi. These industry standards allow communication channels to

be established and maintained between combinations of mobile stations and access points for the transmission of digital information by using techniques such as carrier-sense multiple access protocol with collision avoidance (CSMA/CA) to help provide rapid, equitable connectivity for all stations.

5 Due in part to battery power limitations, the transmission range for reliable communications between mobile stations and access points is limited. Often within a well-configured wireless LAN, a mobile station may be within range of more than one access point, and the access point to which the mobile station connects needs to be determined. For example, mobile station **110** is connected
10 to access point **120**, sometimes referred to as the serving access point. Mobile station **114**, however, may be connected to either access point **120** or access point **124**, with one of the access points **120**, **124** acting as the serving AP while the other is what can be referred to as a neighboring AP. As mobile station **114** moves or roams, or as environmental conditions for radio transmissions change,
15 the serving AP may be changed accordingly.

 Access point **120** has a transmission range **122** within which data transmissions can be sent to and received from one or more mobile stations **110**, **112**, and **114**. Similarly, access point **124** has a transmission range **126** within
20 which data transmissions can be sent to and received from one or more mobile stations **114** and **116**. To begin the process of connecting with a mobile station, an AP transmits, for example, a beacon signal on a prescribed channel. The prescribed channel comprises a prescribed frequency or frequency band that can be received by any mobile station within the transmission range when the mobile station is appropriately tuned and ready to receive the transmission. The beacon
25 signal, commonly referred to as the beacon, comprises, for example, an access-point timestamp, a beacon interval, a basic service set identifier (BSSID), and a traffic indication map (TIM). The access-point timestamp contains timer information from the serving AP such as a copy of the AP's TSF timer to be used for synchronizing time-sensitive operations. The beacon interval indicates the
30 time between two targeted start times of a beacon signal. In one embodiment, the beacon interval is substantially 1024 microseconds. The SSID is an

identifying name assigned to the local network comprising the mobile stations and the APs serving the mobile stations. A BSS is a basic service set that includes a set of stations controlled by a single coordination function. The BSSID in an infrastructure BSS is the MAC address of the serving AP. The traffic indication map, an information element present within beacon frames generated by APs, contains a DTIM count that indicates how many beacons will appear before the next DTIM, a DTIM period indicating the number of beacon intervals between successive DTIMs, a bitmap control field that provides an indication of broadcast or multicast frames buffered at the AP, and a traffic-indication virtual
5 bitmap containing information corresponding to traffic buffered for a specific station within the BSS that the AP is prepared to deliver at the time the beacon frame is transmitted. The DTIM is a beacon signal that contains a delivery traffic information message (DTIM) after which an AP sends out buffered broadcast and multicast media access control (MAC) service data units (MSDU), followed by
10 any unicast frames. The beacon signal may also include within the beacon frame fields containing information such as capability information, supported rates, and parameters related to frequency hopping (FH) or direct sequence spread spectrum (DSSS) physical layers (PHYs).

In addition to beacon signals, gratuitous probe responses (GPRs) may be
20 periodically received at a mobile station from an AP. The received GPR includes, for example, an access-point timestamp, a gratuitous probe response interval, and a basic service set identifier. Similar to the beacon signal, the GPR contains timing and synchronization information from the serving AP though omits the potentially lengthy TIM and other information contained in the beacon
25 frame. Because GPR frames are shorter than beacon frames, transmission and reception of GPR frames lessens the load on the network, and GPRs can be sent much more frequently than beacon signals. Gratuitous probe response frames, sometimes referred to as unsolicited probe responses, contain similar information as probe response frames, though do not require the generation and
30 transmission of an asynchronous probe request frame from the mobile station and contain non-standard information elements such as the GPR interval.

Eliminating the need to send probe requests thereby reduces power consumption within the mobile station. Elimination of probe requests from potentially many mobile stations connected to the AP reduces load on the network and increases overall capacity.

5 The mobile station can reduce its power consumption by generating and executing an enhanced passive scanning schedule that is based on timing information received from beacon signals, probe response, and GPRs, and is stored in its site timing table (STT). The STT has a site timing table entry corresponding to the serving AP and any neighboring APs. For example, a site
10 timing table entry is created or updated by a beacon, probe response, or GPR. The STT is created, for example, by a beacon or a probe response. The STT is updated, for example, using EPS with information received from either a beacon or a GPR. The mobile station receives beacon signals and GPRs from selected channels with a radio transmitter/receiver within the mobile station, and then an
15 AP can be selected and connected to as the serving AP based on collected transmission measurements such as the received signal strength indicator (RSSI) and other AP information from the received beacon signals and GPRs.

 The site timing table entries may be created, updated and removed based on the received beacon signals and GPRs. The STT and the site timing table
20 entries may be created, updated and removed, for example, by a controller and a memory located within the mobile station. Using site timing table entry information in the STT, an enhanced passive scan schedule may be generated. The enhanced passive scan schedule may include a channel number, a local scan start time, and a maximum channel scan time for each site timing table
25 entry. A scan start time is determined and set based on entries in the updated STT. Based on the scan start time, a power mode such as an active mode or a low-power mode may be determined for the mobile station. To minimize power consumption, the mobile station may enter into the low-power mode when sufficient time remains prior to receiving an anticipated beacon signal or GPR.

30 Computer program code for enhanced passive scanning may reside within any suitable computer usable medium such as read-only memory, random

access memory, internal memory, external memory, flash memory, semiconductor memory, magnetic media, optical memory, compact discs, digital versatile discs, a memory storage device, and combinations thereof. A program for enhanced passive scanning may be stored or loaded into a computer usable medium within a mobile station. The program may include code to scan at least one channel for a beacon signal, probe response, or a GPR; to receive beacon signals and GPRs; to create and update an entry in an STT based on the beacon signals, probe responses, and GPRs; to generate an enhanced passive scan schedule; to set a scan start time based on entries in the updated STT; to determine a power mode for the mobile station based on the scan start time; and to select an access point.

FIG. 2 illustrates an enhanced passive scanning system for a wireless local area network, in accordance with another embodiment of the present invention. Enhanced passive scanning system **200** includes a mobile station **210** and an access point **220** that may be connected to other wired or wireless networks. Mobile station **210**, such as a laptop, a personal digital assistant (PDA), a mobile phone, a cellular phone, or other wireless communication device, can communicate with access point **220** to exchange digital information such as data packets, voice-over-IP, network management frames and control messages. The radio transmitter/receiver within the mobile station contains a scanner for scanning one or more channels for beacon signals and GPRs. Mobile station **210** may be fitted with a wireless network interface card (NIC) or have a built-in radio transmitter/receiver to scan and receive a beacon signal or a GPR from access point **220**. Mobile station **210** has suitable hardware and software to create and update a site timing table for generating an enhanced passive scan schedule and setting scan start times for the reception of beacon signals and GPRs, to select an access point when more than one AP is within transmission range, and to determine a power mode for the wireless communication device.

FIG. 3 shows a plot of beacon signals and gratuitous probe responses transmitted from two access points, in accordance with one embodiment of the

present invention at **300**. This exemplary radio transmission **340**, which includes periodic beacon signals **342a**, **342b**, **342c** and **342d** with a beacon interval of about 100 milliseconds, is received from a first access point. Although beacon signals are intended to be transmitted at the end of each beacon interval,

5 individual beacon signals may be delayed because of a transmission of high-priority voice packets or data packets, a transmission of a long frame that extends past a target beacon transmission time (TBTT), or other traffic on the medium. The beacon intervals may range, for example, between one timing unit (TU) of 1,024 microseconds to over 65,000 TUs. As discussed earlier, a short

10 beacon interval is undesirable in some circumstances because of the potentially large size of the beacon TIM and DTIM frames. In this example, beacon signals with DTIM frames are scheduled every three beacon signals, such that beacon signals **342a** and **342d** contain DTIM frames.

In accordance with some protocols, a mobile station may send a probe

15 request to an access point, which in turn sends back a probe response, the request and response thereby enabling synchronization between the mobile station and the access point as well as the broadcasting of multicast and unicast messages. In the case where many mobile stations, such as fifty mobile stations, are being served by a single access point, a large number of probe

20 requests may be generated, which may slow down the network and generate an unnecessary drain of power within the mobile stations. To help conserve battery power and network resources, gratuitous probe responses can be interjected between beacon signals to provide the mobile stations with needed information in a more schedulable manner such that any individual mobile station may be

25 powered up into an active mode to receive a beacon signal or a GPR at a target beacon transmission time or a target gratuitous probe response transmission time.

A series of gratuitous probe responses **344** may be injected periodically between beacon signals on radio transmission **340**. For example, a GPR is

30 transmitted by the serving AP every five or ten milliseconds.

Serving APs and neighboring APs in any network combination may be set to send a GPR at a target GPR transmission time as well as a beacon signal at a target beacon transmission time. The transmission of any individual beacon signal or a GPR may be delayed occasionally, for example, by the transmission of high-priority data or voice packets, with subsequent beacon signals and GPRs transmitted close to the initial target transmission times. For example, radio transmission **346** from a neighboring AP includes beacon signals **348a**, **348b** and **348c** with beacon signal **348c** containing a DTIM frame without injected GPRs, whereas radio transmission **340** from a serving AP includes beacon signals **342** with interjected GPRs **344**. The transmission and reception of beacon signals and GPRs may be established to effectualize a reduction in power consumption and an improvement in network capacity.

FIG. 4 shows a flow diagram of an enhanced passive scanning (EPS) method for a wireless local area network, in accordance with one embodiment of the present invention at **400**. EPS method **400** includes various steps to initiate and operate a wireless communication network using GPRs.

Enhanced passive scanning method **400** may be initiated by first performing an active scan or a passive scan, as seen at block **405**. An active scan includes the mobile station generating probe request frames and processing probe response frames sent from an access point or another mobile station. Passive scanning includes the mobile station listening to a channel for up to a maximum duration defined by a channel time parameter, then scanning on each designated channel for traffic such as a beacon signal or a GPR. The access point is programmed to generate and send a GPR from an access point. After the active or passive scan, at least one beacon signal or GPR is received. The beacon signal includes, for example, an access-point timestamp, a beacon interval, a basic service set identifier, and a traffic indication map. The GPR includes, for example, an access-point timestamp, a GPR interval, and a basic service set identifier. An access point may be selected based on the received beacon signals or GPRs. In a more specific example, the AP is selected based on the signal quality or the signal strength of the received transmissions. When

the AP is selected, the selected AP becomes the serving AP until another AP is selected. In the case of an ad hoc network with two or more mobile stations, one of the mobile stations can be established as the sender of beacon signals and GPRs.

5 A site timing table may be created based on the beacon signals or GPRs and other access point information received during the active or passive scan, as seen at block **410**. The site timing table is created with at least one site timing table entry. In one example, site timing table information is appended to a station management table (SMT) that includes entry management fields, AP selection
10 fields, and status information.

Site timing table information is obtained by tuning the mobile station to an access point channel, receiving a beacon signal or a GPR, collecting transmission measurements of the access point, and storing access point
15 information in the site timing table. Transmission measurements are made, for example, of received signal strength, estimated noise power values, quality-of-service measurements, frame error rates, or other determiners of channel quality and availability.

With information from the site timing table, an enhanced passive scan schedule may be generated, as seen at block **415**. The enhanced passive scan
20 schedule includes, for example, a channel number, a local scan start time, and a maximum channel scan time for each site timing table entry in the site timing table.

An enhanced passive scan is performed with information in the site timing table and the EPS schedule, as seen at block **420**. Channels are scanned for
25 beacon signals and GPRs from APs that are within range of the mobile station.

At the target beacon transmission time or at a target GPR transmission time, at least one channel is scanned for a beacon signal or GPR, as seen at block **425**. The transmitter/receiver in the mobile station is tuned to an access point channel to receive a beacon signal or a GPR. When the
30 transmitter/receiver is powered down, time is allocated to wake up and warm up the radio before the transmitter/receiver receives the beacon signal or GPR at

the target transmission time. When the transmitter/receiver is tuned to the selected channel, a beacon signal or a GPR may be received. When a beacon signal or GPR is received, the next channel may be scanned. The beacon signal or the GPR may be received from an access point or another mobile station in an ad hoc network.

Based on the received beacon signal or GPR, a different access point may be selected, as seen at block **430**. The mobile station is connected to the selected access point. Alternatively, access point selection may occur after creating or updating the site timing table, or at other appropriate points during the EPS. For example, the AP selection may occur upon completion of the EPS to allow for each AP to have an equal chance of being selected.

With information received from the beacon signal or the GPR, entries within the site timing table may be updated, as seen at block **435**. Entries in the site timing table, such as an access-point timestamp, a local station timestamp, a beacon interval or a GPR interval, are updated according to information received from the beacon signal or the GPR. The local station timestamp comprises local station timing information, which may include the time when the first byte of the beacon signal or the GPR frame was received. In some cases, entries within the site timing table will be added when the mobile station comes within the range of another access point. In other cases, site timing table entries will be removed when the mobile station goes out of range of an access point.

The EPS schedule is generated with the updated information in the site timing table, including a channel number, a local scan start time, and a maximum channel scan time for each site timing table entry in the site timing table, as seen at block **440**. The local scan start time can be calculated, for example, from the access-point timestamp, the local station timestamp, and the beacon or GPR interval. The maximum channel scan time may be set differently for each channel, and may be dynamically adjusted while the EPS is performed in order to accommodate, for example, a constantly busy channel or an excessive amount of jitter in the actual beacon signal or GPR transmission time received over a given channel.

Based on entries in the updated site timing table, a scan start time is set, as seen at block **445**. The scan start time may be set, for example, based on the EPS with chronologized channel information such that the next anticipated beacon signal or GPR transmission can be received. A maximum scan time for each channel being scanned may be determined based on entries in the updated site timing table.

A power mode may be determined based on the scan start time, as seen at block **450**. When sufficient time exists prior to the next anticipated beacon signal or GPR transmission, the mobile station may be placed into a low-power mode to minimize power consumption. For example, a calculation is made for a time period remaining until a target beacon transmission time or a target gratuitous probe response transmission time is scheduled. The mobile station may enter a low-power mode based on the calculation and other time considerations such as receiver warm-up time, processor wake-up time, or baseband circuitry warm-up time.

When time allows, the low-power mode is entered, as seen at block **455**. For example, a low-power timer is set based on the scan start time and wake-up time required to receive beacon signals and GPRs. When the low-power timer expires, the mobile station exits the low-power mode. Whether or not the mobile station enters the low-power mode, enhanced passive scanning is continued as seen back at block **420** in accordance with the EPS schedule generated from the site timing table.

FIG. 5 shows a block diagram of an enhanced passive scanning system for a wireless local area network, in accordance with one embodiment of the present invention at **500**. Enhanced passive scanning system **500** includes a mobile station **510**. Mobile station **510** includes a controller **550**, a transmitter/receiver **552**, a pair of diversified antennas **554a** and **554b**, a memory **556**, and a set of timers **558**. Running computer program code stored in memory **556**, controller **550** directs transmitter/receiver **552** to receive beacon signals and GPRs. A site timing table entry in a site timing table stored in memory **556** may be updated based on the received beacon signals or GPRs. A scan start time

may be set and stored in a set of timers **558**. Based on the scan start time, mobile station **510** may determine a power mode and enter into a low-power mode when sufficient time is available before receiving the next beacon signal or GPR.

5 **FIG. 6** shows a block diagram of an enhanced passive scanning system for a wireless local area network, in accordance with another embodiment of the present invention at **600**. Enhanced passive scanning system **600** includes a wireless communication device or mobile station **610**. Mobile station **610** includes a host processor **650**, a WLAN integrated circuit **670**, and an
10 802.11a/b/g radio **692**.

Host processor **650** may be a discrete or an embedded processor for controlling the execution of functions within mobile station **610**. In one example of a function, host processor **650** drives WLAN integrated circuit **670** according to computer program code for enhanced passive scanning stored in a memory **656**.
15 A portion of this code, the WLAN IC driver **660**, drives WLAN integrated circuit **670** accordingly for executing a beacon signal and GPR processing function **662** and for performing other functions such as an enhanced passive scanning function **664**. Beacon signals and GPRs that are received by mobile station **610** may be processed by beacon signal and GPR processing function **662**, with the
20 processed results stored in a site timing table or a database within memory **656**.

An EPS scheduler **666** run by host processor **650** as part of WLAN IC driver **660** generates an EPS schedule based on site timing table entries stored within memory **656**. In one example, the EPS schedule includes a channel number, a local scan start time, and a maximum channel scan time for each site
25 timing table entry in the site timing table. An EPS scan start timer **668** may be used to store a timer value corresponding to a target beacon transmission time or a target GPR transmission time. For example, EPS scan start timer **668** is programmed with a rate at which measurements of the serving and/or neighboring APs are required, such as approximately 500 milliseconds. The
30 timer may be located in an internal register, internal memory, external memory, or other suitable memory location.

Host processor **650** interfaces with WLAN integrated circuit **670** using a 16-bit generic slave interface or other suitable interface such as USB, a serial interface, an RS232 interface, a parallel interface, or a memory-mapped interface, according to appropriate protocols.

5 WLAN integrated circuit **670**, such as the TNETW1220 or TNETW1230 integrated circuit manufactured by Texas Instruments, Inc., includes an embedded central processing unit (CPU) **672** that controls functions being executed such as baseband processing and interfacing functions between WLAN integrated circuit **670** and host processor **650**. For example, a frame process
10 module **674** may receive beacon signals and GPRs and store the results in a memory **676**. Memory **676** may be used to buffer beacon signal, probe response, and GPR frames. An EPS process module **678** may receive information from WLAN IC driver **660** to execute an EPS process. An EPS schedule process module **680** stores timing synchronization function (TSF) timer
15 information from a serving AP into a local TSF timer **682**. A power management process module **684** determines when to enter a low-power mode by setting a low-power timer **686**, entering the low-power mode, and waking up when low-power timer **686** expires. Radio control module **688** receives a channel number and tunes radio **692** according to a local scan start time up to a maximum
20 channel scan time. A channel scan timer **690** may be set by radio control module **688** corresponding to the scan time computed to receive a beacon signal or a GPR. When a beacon signal or GPR is received, radio control module **688** may direct radio **692** to scan another channel. Radio transmissions are sent and received with a pair of diversified antennas **694a** and **694b**.

25 Passive scanning is performed by host process **650** with WLAN IC driver **660**, in coordination with WLAN integrated circuit **670** and radio **692**. In one example, the driver sends a passive scan command with a list of channels to firmware residing within WLAN integrated circuit **670**. The firmware tunes radio **692** to a selected channel that is supported by mobile station **610**. The firmware
30 programs channel scan timer **690** with the maximum time to scan while on the selected channel. Radio **692** listens for beacon signals until time runs out.

When a beacon signal is received, the firmware sends beacon frame information to the driver and the driver records AP site timing information. Each channel in the list is scanned in turn, and an AP is selected from available access points.

5 The driver can dynamically change the value of channel scan timer **690** for each channel to improve the performance of the passive scan. The amount of channel scan time may be calculated by using the timing information from the TSF timer received with the beacon signal from each AP and the local TSF time or local station timestamp stored in local TSF timer **682** in mobile station **610**. The calculation may consider jitter in the beacon signal or GPR. The sequence
10 begins by the driver initiating an active scan to populate the site timing table that includes the channel number, BSSID, access-point timestamp (TSF timer from the AP), and local station timestamp. At the neighboring AP scan rate, the driver initiates an EPS. The driver reads the local station timestamp value to calculate the length of time for a passive scan to receive a beacon signal or GPR from the
15 first AP in the site timing table. The driver commands the firmware to perform a passive scan. The driver receives beacon signals and GPRs from APs within range. The driver proceeds in this manner until all AP site timing table entries have been scanned. As the beacon signals or GPRs are received, the timing information is updated in the site timing table.

20 Another enhancement to passive scanning, the driver waits until the beacon signal or GPR is near to issue an EPS scan command. The value of channel scan timer **690** is set to a constant value for all access points. The amount of time to delay issuing the EPS scan command is calculated, for example, using the timing information from each access-point timestamp and the
25 local station timestamp. The calculation may take into account jitter in the beacon signal or GPR. The sequence begins by the driver initiating an active scan to populate the site timing table that includes a channel number, BSSID, access-point timestamp, and local station timestamp. At the neighboring AP scan rate, the driver initiates an EPS. The driver then reads the local timestamp
30 and access-point timestamp to determine when to send an EPS scan command to the firmware. The driver receives the beacon signal or GPR. The driver

proceeds in this manner until all access points in the site timing table have been scanned. As beacons signals or GPRs are received, the timing information in the site timing table is updated.

To perform an enhanced passive scan, the driver programs EPS scan start timer **668**. When EPS scan start timer **668** expires, the driver creates and sends an EPS command to the firmware. In an exemplary EPS command, the driver sends the number of APs to scan, the EPS schedule for the number of APs to scan, the channel number of AP to scan, the AP scan start time in local TSF timer units, and the maximum scan time to listen for a beacon signal or a GPR. The driver orders the EPS command in chronological order of expected beacon signal or GPR reception times for neighboring APs.

For each access point within range of mobile station **610**, the firmware computes the amount of time remaining before an AP scan start time. If enough time exists to enter a low-power mode, the firmware programs low-power timer **686**. The firmware enters the low-power mode until low-power timer **686** expires, then exits the low-power mode. The firmware tunes radio **692** to a selected channel, programs AP channel scan timer **690**, and listens for beacon signals or GPRs until channel scan timer **690** expires or a beacon signal or GPR is received. While the EPS is in progress, the firmware buffers the received beacon signal and GPR frames, and may send an unsolicited information message to the driver indicating the scan is complete. After all APs are scanned, the driver receives buffered beacon signal and GPR frames for parsing and processing. The driver then updates the site timing table with the received information, selects an appropriate access point, and programs EPS scan start timer **668** with the time remaining until the next EPS scan.

When performing an EPS, the driver may receive a packet for transmission. In this case, the driver determines the type of packet. For a voice packet, the driver sends the packet to the firmware for transmission. The firmware pauses the EPS for the entire duration of the voice frame exchange sequence. Upon completion of the sequence, the firmware resumes the EPS.

The firmware may not be able to resume the EPS with the next neighboring AP when the voice frame exchange sequence is extended due to retransmissions. For data packets, the driver may hold the low priority packets until an unsolicited information message is received from the firmware indicating the EPS is

- 5 complete. When a high priority data packet is received from the driver, the firmware may abort the EPS and transmit the packet. In the event the EPS is aborted by the firmware, the driver can determine which neighboring APs were not scanned and reschedule the EPS.

- 10 While the embodiments of the invention disclosed herein are presently preferred, various changes and modifications can be made without departing from the spirit and scope of the invention. The scope of the invention is indicated in the appended claims, and all changes that come within the meaning and range of equivalents are intended to be embraced therein.

15